State of West Virginia Office of Technology
Policy: Information Security Audit Program
Issued by the CTO

1.0 PURPOSE

The West Virginia Office of Technology (WVOT) will maintain an objective and internally independent Information Security Audit Program. This program will serve the Executive Branch by examining, evaluating, and reporting on information technology (IT) applications, related systems, operations, processes, and practices to provide reasonable assurance that security controls will:

- Safeguard information assets and protect privacy;
- Preserve the integrity and reliability of data;
- Function as intended to achieve the entity's objectives; and
- Comply with established and/or relevant standards, policy, and regulations.

Audit efforts are focused on areas presenting the highest degree of risk, as well as on those areas where risk mitigation will provide the greatest potential benefit to the Executive Branch. This policy explains the authority of the WVOT Information Security Audit Program, as well as the standards of audit practice.

2.0 SCOPE

This policy applies to all State entities or personnel who desire or require auditing services from the WVOT Information Security Audit Program.

3.0 RELEVANT DOCUMENTS/MATERIAL

3.1 WVOT-PR1008 – Information Security Audit Program

3.2 West Virginia Office of Technology (WVOT) Page

3.3 West Virginia Code§5A-6-4a – "Duties of the Chief Technology Officer Relating to Security of Government Information"

3.4 *Proper Use of Government Information, Resources, and Position* (Government Audit Standards, July 2007)

3.5 West Virginia Code §29B-1-4 – Freedom of Information Act Exemptions – Public Records

4.0 POLICY

4.1 Confidentiality

4.1.1 All WVOT IT Auditors are bound by confidentiality standards, and are required to sign the Department of Administration Confidentiality Statement annually.

4.1.2 All WVOT IT Auditors will sign-off on WVOT-PO1001, the *Information Security* policy.

4.1.3 Information collected during an audit will only be used for official purposes and not for personal gain, in a manner contrary to law, or detrimental to the legitimate interests of the audited entity or the audit organization. This includes the proper handling of sensitive or classified information or resources.

4.1.4 The public's right to the transparency of government information must maintain a balance with the proper use of that information. In addition, many government programs are subject to laws and regulations dealing with the disclosure of information. To accomplish the balance, WVOT IT Auditors will exercise discretion in the use of information acquired in the course of duties in achieving this goal. WVOT IT Auditors will not improperly disclose any such information to third parties under any circumstances.

4.2 The WVOT Information Security Audit Program is responsible for providing the following to its customers:

4.2.1 Objective, internally independent examination of security controls pertaining to systems, operations, processes, and practices;

4.2.2 Reasonable assurance that security controls will: (1) safeguard information assets and protect privacy; (2) preserve the integrity and reliability of data; (3) function as intended to achieve the entity's objectives; and (4) operate in accordance with standards, policy, and regulations.

4.2.3 Report threats and vulnerabilities found, including unexpected items and/or situations detected during the audit.

4.2.4 Provide recommendations to mitigate or resolve risk as identified in the audit findings.

4.3 During the period of the audit engagement, in order to obtain accurate and complete information, perform thorough evaluations, and prepare meaningful reports, WVOT Information Security Audit personnel will:

4.3.1 Prepare an engagement memo for the customer with details of audit objectives, scope, and schedule;

4.3.2 Acquire and maintain complete access, on a need to know basis, to records, property, computer systems, functions, and personnel;

4.3.3 Allocate resources, establish schedules, select subjects, determine audit scope, and apply the techniques required to achieve engagement objectives; and

4.3.4 Obtain the necessary assistance of personnel within the units/functions of the agency where they provide services.

4.4 Prior to internal audit engagements, entities/customer must read, agree to comply with, and sign-off on an engagement memo, all provisions of this policy, and WVOT-PR1008, the *Information Security Audit Program* procedure.

4.5 The draft engagement findings and recommendations will be forwarded to the client Director.

4.6 The delivery of the final engagement findings and recommendations will be limited to the CTO, the CISO, the client Director, and other parties as authorized.

4.7 The Information Security Audit Program will only release engagement findings and recommendations to additional entities under the following circumstances: by request from the audit client, for peer review, and/or under order of subpoena. Only Information specific to the request will be released.

4.8 Internal audit reports are exempt from disclosure under the West Virginia's Freedom of Information Act (West Virginia Code §29B-1-4). Examples of exemptions include internal memoranda or letters received or prepared by any public body; records containing specific or unique vulnerability assessments or specific or unique response plans, data, or databases; computing or telecommunications and network security records, passwords, etc.; security or disaster recovery plans, risk assessments, tests or the results of those tests, etc.

4.9 Information Security Audits may be scheduled in relationship to the following:

4.9.1 Scheduled at least three (3) to six (6) months in advance (see WVOT-PR1008);

4.9.2 On an ad-hoc basis;

4.9.3 As a client special request;

4.9.4 Post incident; or

4.9.5 As a risk assessment;

5.0 STANDARD PRACTICES

5.1 Standards of Audit Practice

5.1.1 The WVOT Office of Information Security and Controls (OISC) has undertaken the establishment, maintenance, and management of an internal Information Security Audit Program.

5.1.2 The WVOT Information Security Audit Program follows the Professional Standards of the Practice of Internal Auditing as issued by the Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), and the International Information Systems Security Certification Consortium (ISC²) Additionally, the WVOT Audit Program adheres to information security standards as published by the Information Standards Organization (ISO).

5.1.3 The Information Security Audit Program will present a rolling Three Year Audit Plan to the Information Security Audit Committee. This reporting relationship will provide internal independence from the departments and activities under review, demonstrate administrative support for the Information Security Audit Program, and ensure adequate consideration of audit findings and recommendations.

5.2 Types of Information Security Audits

5.2.1 The types of audits performed by the Program include, but are not limited to the following:

- Account Management
- Application Controls
- Business-Technical Processes

- Certification and Accreditation
- Change Control
- Configuration Management
- Control Procedures and Practices
- Data Centers/Facilities
- Data Management
- Desktop Practices
- Disaster Recovery
- End of Life Procedures
- Incident Management
- Internal Controls for Technology
- Mobile Devices and Media
- Networks
- Policy and Regulatory Compliance
- Servers
- Technology Acquisitions
- Telecommunications
- Other Resources

5.3 Third Party Audits

5.3.1 Agencies engaging in any IT audit activity with third parties are responsible for contacting the WVOT OISC Audit Team as soon as notification of the audit has been received.

5.3.2 The WVOT Information Security Audit Program will coordinate third-party information security audit activities. This coordination will:

5.3.2.1 Determine that audit objectives are clearly defined, and then achieved upon completion. This will include a review of the engagement memo;

5.3.2.2 Ensure that appropriate and accurate information is provided to third-party auditors;

5.3.2.3 Avoid duplicate audits and control audit costs;

5.3.2.4 Ensure that operating units cooperate fully with the third-party auditors;

5.3.2.5 Coordinate communications between Executive Branch personnel and third-party auditors including, but not limited to audit findings and recommendations;

5.3.2.6 Review engagement findings and recommendations; and

5.3.2.7 Facilitate effective follow-up activities and monitor progress in addressing audit recommendations.

5.3.3 Third-party auditors may be required to follow additional and/or more stringent standards and procedures than those mandated by the WVOT.

6.0 ENFORCEMENT

Any individual or agency found to have violated the provisions of this policy may be subject to an accountability review by Department and/or State leadership. Any action, if determined to be necessary, will be administered by the appropriate authority and may be based on recommendations of the West Virginia Division of Personnel, intended to address severity of the violation and the consistency of sanctions.

7.0 LEGAL AUTHORITY

Under the provisions of West Virginia Code §5A-6-4a *et seq*., the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

8.0 DEFINITIONS

8.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

8.2 Information Security Audit Committee - A committee, with representation from the GIEST and WVOT, that serves to review significant audit findings and audit plans to ensure that current, information security risks are considered during audit planning and that risks with enterprise-wide impact are adequately addressed.

8.3 Information Security Audit Program - The types of audits performed by the Program include, but are not limited to the following: (1) Applications and systems; (2) Data centers /sites; (3) Data management; (4) Internal technology controls; (5) Investigative and incident follow-up; (6) Mobile and portable devices; (7) Networks and network components; (8) Physical security; (9) Policy and regulatory compliance; (10) Telecommunications; and (11) Technology operations. OISC Auditors serve the Executive Branch by examining, evaluating, and reporting on IT applications, systems, operations, processes, and practices to provide reasonable assurance that security controls:

- Safeguard information assets and protect privacy
- Preserve the integrity and reliability of data
- Function as intended to achieve the entity's objectives
- Operate in accordance with standards, policy, and regulations

8.4 Information Systems Audit and Control Association (ISACA). An International professional organization that establishes standards for the practice of Information Technology Auditing. ISACA also manages certification/licensing exams, continuing education for Certified Information Security Auditors, Certified Information Security Managers and other security professionals. ISACA is a global organization for information governance, control, security and audit professionals.

8.5 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

8.6 Institute of Internal Auditors (IIA) – An international professional association, which is recognized throughout the world as the internal audit profession's leader in certification, education, research, and technical guidance. The mission of the association is to provide dynamic leadership for the global profession of internal auditing. Members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

8.7 Integrity - Protecting data from unauthorized or unintentional modification or deletion.

8.8 International Information Systems Security Certification Consortium (ISC²) -The International Information Systems Security Certification Consortium, Inc. [(ISC) ²] is a not-for-profit organization incorporated under the laws of the Commonwealth of Massachusetts and the U.S. Internal Revenue Code. As such, all credential holders in good standing are considered members of (ISC) ². (ISC) ² is charged with the responsibility for maintaining the (ISC) ² CBK®, a compendium of industry best practices for information security, including those for CISSPs, SSCPs, and CAPs. The CBK is a critical component for certifying the minimum acceptable competence for professionals seeking to hold various credentials. (ISC) ² also provides the information security community with education seminars, examinations and related services. In addition, (ISC) ² acts to safeguard certification standards, and participates in information security conferences, etc., as some of its more important activities.

8.9 Office of Information Security and Controls (OISC) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.

8.10 Three-Year Security Audit Plan – A rolling plan developed by the Information Security Audit Program to schedule audits and select audit targets. This plan will be reviewed and revised annually by the Chief Information Security Officer (CISO) and the Information Security Audit Committee.

8.11 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.*, which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

9.0 INDEX

E

I

O

P

R

S

Policy: Information Security Audit Program

State of West Virginia Office of Technology